FORM PTO-1390 (REV. 11-2000) U S DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE

TRANSMITTAL LETTER TO THE UNITED STATES DESIGNATED/ELECTED OFFICE (DO/EO/US) CONCERNING A FILING UNDER 35 U.S.C. 371

ATTORNEY 'S DOCKET NUMBER: PTT-111(402548US)

U S APPLICATION NO (If known, see 37 CFR 1 5): 09/787648

INTERNATIONAL APPLICATION NO.	INTERNATIONAL FILING DATE	PRIORITY DATE CLAIMED
PCT/EP99/10208	16 December 1999	30 December 1998

TITLE OF INVENTION: METHOD AND DEVICE FOR CRYPTOGRAPHICALLY PROCESSING DATA

APPLICANT(S) FOR DO/EO/US: ROELOFSEN, Gerrit; VAN BRUCHEM, Dirk Jan Jacobus; MULLER, Frank; ROMBAUT, Willem

Applicant herewith submits to the United States Designated/Elected Office (DO/EO/US) the following items and other information:

1. [X] This is a **FIRST** submission of items concerning a filing under 35 U.S.C. 371.
2. [ ] This is a **SECOND** or **SUBSEQUENT** submission of items concerning a filing under 35 U.S.C. 371.
3. [X] This is an express request to begin national examination procedures (35 U.S.C. 371(f)). The submission must include items (5), (6), (9) and (21) indicated below.
4. [X] The US has been elected by the expiration of 19 months from the priority date (Article 31).
5. [ ] A copy of the International Application as filed (35 U.S.C. 371(c)(2))
   a. [ ] is attached hereto (required only if not communicated by the International Bureau).
   b. [ ] has been communicated by the International Bureau.
   c. [ ] is not required, as the application was filed in the United States Receiving Office (RO/US).
6. [ ] An English language translation of the International Application as filed (35 U.S.C. 371(c)(2)).
   a. [ ] is attached hereto.
   b. [ ] has been previously submitted under 35 U.S.C. 154(d)(4).
7. [ ] Amendments to the claims of the International Aplication under PCT Article 19 (35 U.S.C. 371(c)(3))
   a. [ ] are attached hereto (required only if not communicated by the International Bureau).
   b. [ ] have been communicated by the International Bureau.
   c. [ ] have not been made; however, the time limit for making such amendments has NOT expired.
   d. [ ] have not been made and will not be made.
8. [ ] An English language translation of the amendments to the claims under PCT Article 19 (35 U.S.C. 371 (c)(3)).
9. [X] An oath or declaration of the inventor(s) (35 U.S.C. 371(c)(4)). (6 pps.)
10. [ ] An English lanugage translation of the annexes of the International Preliminary Examination Report under PCT Article 36 (35 U.S.C. 371(c)(5)).

Items 11 to 20 below concern document(s) or information included:

11. [X] An Information Disclosure Statement under 37 CFR 1.97 and 1.98. (with modified Form PTO/SB/08A, copy of International Search Report, Dutch Search Report and Six (6) cited references)
12. [X] An assignment document for recording. A separate cover sheet in compliance with 37 CFR 3.28 and 3.31 is included. (4 pps.)
13. [X] A FIRST preliminary amendment. (with clean set of claims)
14. [ ] A SECOND or SUBSEQUENT preliminary amendment.
15. [ ] A substitute specification.
16. [ ] A change of power of attorney and/or address letter.
17. [ ] A computer-readable form of the sequence listing in accordance with PCT Rule 13ter.2 and 35 U.S.C. 1.821 - 1.825.
18. [ ] A second copy of the published international application under 35 U.S.C. 154(d)(4).
19. [ ] A second copy of the English language translation of the international application under 35 U.S.C. 154(d)(4).
20. [X] Other items or information:
    Postcard receipt, Cover Letter, International Publication No. WO 00/41356 (including seven (7) formal drawing sheets [1-10], Notification of Transmittal of the International Preliminary Examination Report with IPEA and amended sheets (11 pps.), Request (8 pps.), Notification of International Application Number (1 pp.), Demand (6 pps.), Submission of Priority Document with certified copy (and English translation) of Netherlands Appl. 1010921 (12/30/98); Netherlands Appl. 1011800 (4/15/99); and Netherlands Appl. 1011544 (3/12/99).

U.S. APPLICATION NO (If known, see 37 CFR 1.5)	INTERNATIONAL APPLICATION NO	ATTORNEY'S DOCKET NUMBER
09/787648	PCT/EP99/10208	PTT-111(402548US)

21. [X] The following fees are submitted:

BASIC NATIONAL FEE (37 CFR 1.492 (a) (1) - (5)):

		CALCULATIONS PTO USE ONLY
Neither international preliminary examination fee (37 CFR 1.482) nor international search fee (37 CFR 1.445(a)(2)) paid to USPTO and International Search Report not prepared by the EPO or JPO	**$1000.00**	
International preliminary examination fee (37 CFR 1.482) not paid to USPTO but International Search Report prepared by the EPO or JPO	**$860.00**	
International preliminary examination fee (37 CFR 1.482) not paid to USPTO but international search fee (37 CFR 1.445(a)(2)) paid to USPTO	**$710.00**	
International preliminary examination fee (37 CFR 1.482) paid to USPTO but all claims did not satisfy provisions of PCT Article 33(1)-(4)	**$690.00**	
International preliminary examination fee (37 CFR 1.482) paid to USPTO and all claims satisfied provisions of PCT Article 33(1)-(4)	**$100.00**	
ENTER APPROPRIATE BASIC FEE AMOUNT =		$ 860.00
Surcharge of **$130.00** for furnishing the oath or declaration later than [ ] 20 [ ] 30 months from the earliest claimed priority date (37 CFR 1.492(e)).		$ 00.00

CLAIMS	NUMBER FILED	NUMBER EXTRA	RATE	
Total claims	25 - 20 =	5	x **$18.00**	$ 90.00
Independent claims	4 - 3 =	1	x **$80.00**	$ 80.00
MULTIPLE DEPENDENT CLAIM(S) (if applicable)			+ **$270.00**	$ 00.00
TOTAL OF ABOVE CALCULATIONS =				$ 1,030.00
[ ] Applicant claims small entity status. See 37 CFR 1.27. The fees indicated above are reduced by 1/2.			+	$ 00.00
SUBTOTAL =				$ 1,030.00
Processing fee of **$130.00** for furnishing the English translation later than [ ] 20 [ ] 30 months from the earliest claimed priority date (37 CFR 1.492(f)).				$ 00.00
TOTAL NATIONAL FEE =				$ 1,030.00
Fee for recording the enclosed assignment (37 CFR 1.21(h)). The assignment must be accompanied by an appropriate cover sheet (37 CFR 3.28, 3.31). **$40.00** per property +				$ 40.00
TOTAL FEES ENCLOSED =				$ 1,070.00
			Amount to be refunded:	$
			charged:	$

a. [X] A check in the amount of $ 1,070.00 to cover the above fees is enclosed.

b. [ ] Please charge my Deposit Account No. _____ in the amount of $ _____ to cover the above fees. A duplicate copy of this sheet is enclosed.

c. [X] The Commissioner is hereby authorized to charge any additional fees which may be required, or credit any overpayment to Deposit Account No. 13-3083 . A duplicate copy of this sheet is enclosed.

d. [ ] Fees are to be charged to a credit card. **WARNING:** Information on this form may become public. **Credit card information should not be included on this form.** Provide credit card information and authorization on PTO-2038.

NOTE: Where an appropriate time limit under 37 CFR 1.494 or 1.495 has not been met, a petition to revive (37 CFR 1.137 (a) or (b)) must be filed and granted to restore the application to pending status.

SEND ALL CORRESPONDENCE TO:
Peter L. Michaelson
MICHAELSON & WALLACE
Parkway 109 Office Center
328 Newman Springs Road
P.O. Box 8489
Red Bank, NJ 07701

SIGNATURE

Peter L. Michaelson
NAME

30.090
REGISTRATION NUMBER

Customer No. 007265

(PTT111TRANS/69:ca)

IN THE UNITED STATES
RECEIVING OFFICE (RO/US)

Inventors: **ROELOFSEN, Gerrit; VAN BRUCHEM, Dirk Jan Jacobus; MULLER, Frank; ROMBAUT, Willem**

International Application No.: **PCT/EP99/10208**

International Filing Date: **16 December 1999**

Priority Claimed: **30 December 1998**
12 March 1999
15 April 1999

Atty. Doc.: **PTT-111(402548US)**

Title: **METHOD AND DEVICE FOR CRYPTOGRAPHICALLY PROCESSING DATA**

COMMISSIONER FOR PATENTS
BOX PCT
Washington, D. C. 20231

S I R:

PRELIMINARY AMENDMENT

Please amend the above-identified patent application which is simultaneously filed herewith, as follows:

IN THE CLAIMS-

To facilitate entry of the following changes, the Applicants have also submitted herewith substitute pages providing all the pending claims, as they now stand, incorporating the changes indicated below.

Amend the following claims:

-- 1. (amended) Method for cryptographically processing data, comprising feeding, to a cryptographic process (P), values, namely, the data (X) and a key (K), and carrying out the process (P) in order to form cryptographically processed output data (Y), [characterised] characterized by feeding, to the process (P), auxiliary values (K*; A, B) and compensating, by an auxiliary process, the influence of the auxiliary values to the output data, in order to mask the values (K; D) used in the process (P). --.

Claim 4,	line 1	Delete "or 3";
Claim 5,	line 1	Delete "3 or 4,";
Claim 7,	line 1	Change "any of the claims 2-6" to --claim 2--;
Claim 8,	line 1	Change "any of the preceding claims" to --claim 1--;
Claim 10,	line 1	Delete "or 9";
Claim 12,	line 1	Change "claims 10 and 11" to --claim 11--;
Claim 13,	line 1	Change "any of the claims 8-12" to --claim 8--;
Claim 14,	line 1	Change "any of the claims 9-13" to --claim 9--;
Claim 16,	line 1	Delete "or 15";

Claim 18, line 1	Change "any of the claims 8-17" to --claim 8--;
Claim 20, line 1	Change "any of the claims 8-19" to --claim 8--;
Claim 21, line 1	Change "any of the preceding claims" to --claim 1--;
Claim 22, line 1	Change "any of the preceding claims" to --claim 1--; and
Claim 23, lines 1-2	Change "any of the preceding claims" to --claim 1--.

REMARKS

The foregoing amendment is made to conform the claims in the application to that amended in the International Preliminary Examination Report and to delete multiple dependent claims.

Respectfully submitted,

19 March 2001

Peter L. MICHAELSON, Attorney
Reg. No. 30,090
Customer No. 007265
(732) 530-6671

MICHAELSON & WALLACE
Counselors at Law
Parkway 109 Office Center
328 Newman Springs Road
P.O. Box 8489
Red Bank, New Jersey 07701

*****EXPRESS MAIL CERTIFICATION*****

"Express Mail" mailing label number: **EL632364167US**
Date of deposit: **20 March 2001**

I hereby certify that this paper or fee is being deposited with the United States Postal Service "Express Mail Post Office to Addressee" service under 37 CFR 1.10 on the date indicated above and is addressed to the Commissioner for Patents, **Box PCT**, Washington, D.C. 20231.

Peter L Michaelson
Signature of person making certification

Peter L. MICHAELSON
Name of person making certification

(PTT111PREAMD/69:ca)

CLAIMS

1. Method for cryptographically processing data, comprising feeding, to a cryptographic process (P), values, namely, the data (X) and a key (K), and carrying out the process (P) in order to form cryptographically processed output data (Y), characterized by feeding, to the process (P), auxiliary values (K*; A, B) and compensating, by an auxiliary process, the influence of the auxiliary values to the output data, in order to mask the values (K; D) used in the process (P).

2. Method according to claim 1, wherein an auxiliary value comprises a supplementary key (K*) which is fed to a supplementary process (P*) in order to form the key (K).

3. Method according to claim 2, wherein the supplementary process (P*) comprises a cryptographic process to which an auxiliary key (K') is fed.

4. Method according to claim 2, wherein the supplementary process (P*) is an invertible process.

5. Method according to claim 2, wherein the data (X) is also fed to the supplementary process (P*).

6. Method according to claim 5, wherein carrying out the supplementary process (P*) takes place exclusively if the data (X) has predetermined properties.

7. Method according to claim 2, wherein the process (P) and the supplementary process (P*) each are built up from a number of steps, and wherein steps of the process (P) and the supplementary process (P*) are alternated.

8. Method according to claim 1, wherein the process (P) comprises a number of steps (S_i), each having a cryptographic operation (F_i, F_i', F_i'') for processing right-hand data (RD_i) derived from the data (X) and a combinatory operation (C_i) for combining with left-hand data (LD_i) also derived from the data (X), the processed right-hand data (FD_i) in order to form modified left data (SD_i), and wherein the right-hand data (RD_1) is combined with a primary auxiliary value (A_1) prior to the first step (S_1) and the left-hand data (LD_1) is combined with an additional auxiliary value (A_0).

9. Method according to claim 8 wherein, immediately after the last step (S_n), the right-hand data (RD_n) is combined with a further primary auxiliary value (A_n) and the modified left-hand data (SD_n') is combined with a further additional auxiliary value (A_{n+1}).

10. Method according to claim 8, wherein the right-hand data (RD_i) is combined, in each step (S_i) and prior to the operation (F_i'), with the primary auxiliary value (A_i) of said step (S_i).

11. Method according to claim 10, wherein the processed right-hand data (FD_i) is combined, following the operation (F_i), with the secondary auxiliary value (B_i) of said step (S_i).

12. Method according to claim 11, wherein the secondary auxiliary value (B_i) of a step (S_i) is formed from the combination of the primary auxiliary value (A_{i-1}) of the preceding step and the primary auxiliary value (A_{i+1}) of the next step.

13. Method according to claim 8, wherein all primary auxiliary values (A_i) are equal.

14. Method according to claim 9, wherein the primary auxiliary values (A_i) and/or secondary auxiliary values (B_i) have each time been combined with the respective operation (F_i) in advance.

15. Method according to claim 14, wherein a combined operation (F_i') contains several tables, and wherein the tables are determined in a different order each time the process (P) is carried out.

16. Method according to claim 14, wherein a combined operation (F_i') contains several tables, and wherein the elements of the tables are determined and/or stored in a different order each time the process (P) is carried out.

17. Method according to claim 16, wherein the order is stored as a lookup table for the benefit of reading out the elements.

18. Method according to claim 8, wherein the right-hand data (RD_i) is combined with a tertiary auxiliary value (W_i) after each step (S_i).

19. Method according to claim 18, wherein the tertiary auxiliary value (W_i) in all steps, except the last one (S_n) is equal to the combination of the primary auxiliary value (A_1) of the first step (S_1) and the additional auxiliary value (A_0), and in the last step (S_n) is equal to zero.

20. Method according to claim 8, wherein combining is carried out using an XOR operation.

21. Method according to claim 1, wherein the data (X) comprises identification data of a payment means (1) and the processed data (Y) forms a diversified key.

22. Method according to claim 1, wherein the process (P) comprises DES, preferably triple DES.

23. Circuit (10) for carrying out the method according to claim 1.

24. Payment card (1), provided with a circuit (10) according to claim 23.

25. Payment terminal (2) provided with a circuit (10) according to claim 23.

Method and device for cryptographically processing data.

BACKGROUND OF THE INVENTION

The invention relates to a method for cryptographically processing data, comprising feeding, to a cryptographic process, values, namely, the data and a key, and carrying out the process in order to form cryptographically processed data. Such method is generally known.

For cryptographically processing data, in practice there are often applied generally known processes. Examples of such cryptographic processes (algorithms) are DES and RSA [DES = Data Encryption Standard and RSA = Rivest, Shamir & Adleman], which are described, e.g., in the book "Applied Cryptography" by B. Schneier (2nd edition), New York, 1996.

Said processes are published since it was assumed that, in the event of sufficiently large key lengths, it would be impossible, on the basis of the processed data, to retrieve the original data and/or the key, even if the cryptographic process were known.

However, Cryptographic algorithms can be attacked -the goal always is to find the encryption key in use- in different ways:
(1) Mathematical attacks like differential and linear cryptanalysis;
(2) Hardware oriented attacks, called "Side Channel Attacks", viz. attacks based on power consumption analysis or I/O timing analysis.

US-A-5745577 discloses a method for advanced key scheduling of a secret key. The aim is to offer a protection against said mathematical attacks (differential and linear cryptanalysis) by amending the encryption algorithm. Amending the algorithm will cause change of its output and thus the disclosed method does not present any improvement against said "Side Channel Attacks".

SUMMARY OF THE INVENTION

The present invention aims to improve the protection of a cryptographic device against "Side Channel Attacks". In short, said improvement is achieved by masking the data and/or the key by means of generating extra, auxiliary input (data or key) and compensating its influence to the output by adding, to the "main" encryption process, an auxiliary (compensating) process. By said masking measures it will be much more difficult to derive the value of data or key from the behaviour of the power consumption of the cryptographic device (see page 1 lines 32-34). Said

masking, however, happens in such a way that the result of the porcess as a whole remains unchanged: with the same input and key the amended algorithm results into the same, unchanged output.

Thus the invention present a method of the type referred to in the preamble according to the invention which is characterised by feeding, to the process, auxiliary values, while compensating, by means of an auxiliary process, the influence of the auxiliary values to the output data, in order to mask the values used in the process.

By masking the date and/or key(s) it becomes considerably more difficult to derive said values on the basis of the behaviour of the process. The result of the process, i.e., the collection of processed data, in the event of a suitable choice of the auxiliary values may be unchanged, i.e., identical to the result of the process, if no auxiliary values have been fed to it. In this connection, an "auxiliary value" is understood to mean a value (data or key) which is fed to the process as a supplement to the corresponding data and key.

The invention is therefore based on the insight that the derivation of the values used in a cryptographic process is rendered considerably more difficult if said values are masked using said auxiliary values and said auxiliary process.

The invention is partly based on the further insight that the use of auxiliary values does not necessarily affect the outcome of the process.

In a first embodiment of the invention, an auxiliary value comprises a supplementary key which is fed to a supplementary process in order to form the key.

By applying a combination of a known process and a supplementary process, there is formed a new cryptographic process, unknown per se, even if the supplementary process is also known per se.

By deriving the key used for the known process (primary key) from a supplementary key (secondary key) using a supplementary process, there is achieved that not the (primary) key of the known process but the supplementary (secondary) key is offered to the combination of processes. In other words, externally the supplementary (secondary) key, and not the real (primary) key of the process proper, is used. Derivation of the key from the original data and the processed data has thereby become impossible. In addition, the derivation of the

If, e.g., a first device gives off a (supplementary) key which is applied in a second device according to the invention, then in the first device there may be used the inverse of the supplementary process to derive the supplementary key from the original key. In other words, although in both the first and the second device internally the original (primary) key is used, there is exchanged, between the devices, the supplementary (secondary) key. Intercepting the supplementary key, however, does not result in knowledge of the original key.

It may be advantageous if carrying out the supplementary process takes place exclusively if the data has predetermined properties. In this manner, cryptographic processing may be carried out for specific, selected data only, while such is blocked for all other data. In this manner, there is achieved a supplementary protection.

An optimum security is provided if the process and the supplementary process are each constructed of several steps and in which there are alternately carried out steps of the process and the supplementary process. As a result, the properties of the known process are further veiled, as a result of which the derivation of the keys is further complicated.

In a second embodiment of the invention, the process comprises several steps, each of which has a cryptographic operation for processing right-hand data derived from the data and a combinatory operation for combining, with the left-hand data derived from the data, the processed right-hand data in order to form modified left-hand data, in which the right-hand data, prior to the first step, is combined with a primary auxiliary value and the left-hand data is combined with an additional auxiliary value. As a result, the data used in the steps and transferred between the steps is masked.

In order to make it possible for the primary and additional auxiliary values do not make themselves felt in the end result of the process, the right-hand data is combined, preferably immediately after the last step, with a further primary auxiliary value, and the modified left-hand data is combined with a further additional auxiliary value.

In order not to have the result of the operations affected by the primary auxiliary values, the method according to the invention is preferably carried out in such a manner that the right-hand data, in each step and prior to the operation, is combined with the primary auxiliary value of said step.

A further protection is achieved if the processed right-hand data, following the processing, is combined with a secondary auxiliary value of said step.

The secondary auxiliary value of a step is advantageously formed from the combination of the primary auxiliary value of the preceding step and the primary auxiliary value of the next step. As a result, it becomes possible to compensate the auxiliary value in the repeatedly next step, as a result of which said auxiliary value will not make itself felt in the end result of the process.

It is possible to carry out the method according to the invention in such a manner, that all primary auxiliary values are equal. As a result, a very simple practical realisation is possible. The use of several auxiliary values, which are preferably random numbers and are generated anew for each time the process is carried out, however, offers a greater cryptographic security.

A further simplification of said embodiment may be obtained if the primary auxiliary values and/or secondary auxiliary values repeatedly have been combined in advance with the operation in question. This is to say, combining with auxiliary values is processed in the operation in question (e.g., a substitution), in such a manner that the result of the operation in question is equal to that of the original operation plus one or two combinatory operations with auxiliary values. By in advance including in the operation the combinatory operations, a more simple and faster practical realisation is possible.

Said combinatory operations are preferably carried out using an XOR operation [XOR = eXclusive OR]. Other combinatory operations, however, such as binary adding, are basically possible as well.

The invention further provides a circuit for carrying out a method for cryptographically processing data. In addition, the invention supplies a payment card and a payment terminal provided with such circuit.

Below, the invention will be further explained on the basis of the exemplary embodiments shown in the figures.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 schematically shows a cryptographic process according to the prior art.

FIG. 2 schematically shows a first cryptographic process according to a first embodiment of the invention.

FIG. 3 schematically shows a second cryptographic process according to a first embodiment of the invention.

FIG. 4 schematically shows a way in which the processes of figures FIG. 1 and 2 may be carried out.

FIG. 5 schematically shows a cryptographic process having several steps according to the prior art.

FIG. 6 schematically shows a first cryptographic process according to a second embodiment of the invention.

FIG. 7 schematically shows a second cryptographic process according to a second embodiment of the invention.

FIG. 8 schematically shows a third cryptographic process according to a second embodiment of the invention.

FIG. 9 schematically shows a circuit in which the invention is applied.

FIG. 10 schematically shows a payment system in which the invention is applied.

PREFERRED EMBODIMENTS

A (cryptographic) process P according to the prior art is schematically shown in FIG. 1. To the process P, there are fed input data X and a key K. On the basis of the key K, the process P converts the input data X into (cryptographically) processed output data Y: $Y = P_K(X)$. The process P may be a known cryptographic process, such as DES (Data Encryption Standard), triple DES, or RSA (Rivest, Shamir & Adleman).

If the input data X and the output data Y are known, it is basically possible to derive the key K used. In the event of a key of sufficient length (i.e., a sufficient number of bits), it was so far deemed impossible to derive said key, even if the process P were known. Impossible in this case is to say that in theory it is admittedly possible, e.g., by trying out all possible keys, to retrieve the key used, but that such requires an impossibly long computational time. Such "brute-force attack" is therefore hardly a threat to the cryptographic security.

Attacks recently discovered, however, make use of knowledge of the process, as a result of which the number of possible keys may be reduced drastically. Deriving the key K used and/or the input data X from the output data Y therefore becomes possible within acceptable computational times.

The principle of the invention, whose object it is to render such attacks considerably more difficult and time-

consuming, is schematically shown in FIG. 2. Just as in FIG. 1, to a (known) process P there are fed input data X and a (secret) key K to generate output data Y.

Contrary to the situation of FIG. 1, in the situation of FIG. 2 the key K is fed to the process P from a supplementary process P*. The supplementary process P* has a supplementary (secondary) key K* as input data to produce, under the influence of an auxiliary key K', the (primary) key K as output data. The key K is therefore not fed, as is the case in the situation of FIG. 1, from an external source (e.g., a memory) to the process P, but is produced by the process P* from the supplementary (secondary) key K*:

$$K = P^*_{K'}(K).$$

It is therefore the secondary key K*, instead of the primary key K, which is predetermined and stored, e.g., in a key memory (not shown). According to the invention, the primary key K, which is fed to the process P, is not predetermined.

The auxiliary key K' may be a permanently stored, predetermined key. It is also possible to apply a supplementary process P* in which no auxiliary key K' is used.

The combination of the processes P and P* forms a new process which is schematically designated by Q. To the process Q which, on account of the supplementary process P*, is unknown per se, the input data X and the (secondary) key K* are fed to produce the output data Y. The relationship between the secondary key K* and the primary key K is veiled by the supplementary process P*.

The supplementary process P* preferably is the inverse of another, invertible process R. This is to say:

$$P^* = R^{-1}.$$

This enables producing the secondary key K* from the primary key K using R and the auxiliary key K':

$$K^* = R_{K'}(K),$$

as will be further explained later by reference to FIG. 5. The new process Q may possibly be extended by the process R, in such a manner that the primary key K, instead of the secondary key K*,

is fed to the process Q. The primary key K in this case in the process Q is derived from:

$$K = P^*_{K'}(K^*) = P^*_{K'}(R_{K'}(K)).$$

This enables using the same (primary) key as in the prior art.

The cryptographic process Q according to the invention, schematically shown in FIG. 3, also comprises a process P having a primary key K and a supplementary process P* having an auxiliary key K', the primary key K being derived from the supplementary key K* by the supplementary process P*. Supplementing the process of FIG. 1, in this case the input data X is also fed to the supplementary process P*, in such a manner that the primary key K is determined partly as a function of the input data X:

$$K = P^*_{K'}(K^*, X).$$

As a result, there is obtained a supplementary cryptographic protection. In addition, as a result the possibility is offered to carry out the supplementary process P* exclusively if certain input data is offered. This is to say that the supplementary process P* may comprise a test of the input data X, and carrying out the supplementary process P* may depend on the result of said test. Thus, the supplementary process P*, e.g., may be carried out only if the last two bits of the input data X equal zero. The effect of such an input data-dependent operation is that only for certain input data X the correct primary key K will be produced in such a manner that only said input data will deliver the desired output data Y. It will be understood that as a result the cryptographic security is further enhanced.

FIG. 4 schematically shows the way in which substeps of the processes P and P* may be carried out alternatingly ("interleaving") in order to further enhance the protection against attacks. The substeps may include so-called "rounds", such as, e.g., in the case of DES. The substeps, however, preferably comprise only one or a few instructions of a program, with which the processes are being carried out.

In a first step 101, there is carried out a first substep P_1 of the process P. Subsequently, in a second step 102, the first substep P_1* of the supplementary process P* is carried out.

Likewise, in a third step 103, the second substep P_2 of the process P is carried out etc. This continues until, in step 110, the last substep P_n^* of the supplementary process P* has been carried out, it being assumed, for the sake of the example, that the processes P and P* comprise an equal number of substeps. If such is not the case, in step 110 there is carried out the last corresponding substep, and in further steps the remaining substeps are carried out.

By alternating the substeps of the process P, which is known per se, and the process P* (possibly known per se as well), there may be obtained a series of substeps which does not correspond to that of a known process. As a result, the nature of the process is more difficult to recognise.

The cryptographic process P schematically shown, only by way of example, in FIG. 5, according to the prior art comprises several steps S_i (i.e., S_1, S_2, ..., S_n). In each step S_i, (right-hand) data RD_i is fed to a cryptographic operation F_i. Said cryptographic operation may itself comprise a number of substeps, such as an expansion, a combination with a key, a substitution and a permutation which, however, have not been designated separately for the sake of the simplicity of the drawing. The cryptographic operation F_i provides processed data FD_i:

$$FD_i = F_i(RD_i).$$

In a combinatory operation CC_i (CC_1, CC_2, ..., the index i always indicating the step S in question), the processed data FD_i is combined with left-hand data LD_i to form modified (left-hand) data SD_i which, just as the original right-hand data RD, is passed on to the next step. The combinatory operations CC_i preferably are XOR operations (symbol: $\oplus$).

As is shown in FIG. 5, at the end of each step S_i the modified left-hand data SD_i and the right-hand data RD_i change positions in such a manner that they form the right-hand data RD_{i+1} and the left-hand data LD_{i+1} of the next step S_{i+1}.

The left-hand data LD_1 and the right-hand data RD_1 of the first step S_1 were derived, in a preceding operation, from input data X and, in doing so, may undergo a preparatory processing, such as an input permutation. The output data SD_n and RD_n of the last step S_n form the processed data Y of the proces P, possibly after it has undergone a final operation, such as an output permutation PP^{-1}.

The cryptographic process of FIG. 6 largely corresponds to that of FIG. 5. In accordance with the invention, the data present in and between the steps is masked with auxiliary values. For this purpose, in this embodiment the first step S_1 is preceded by (preparatory) combinatory operations DC and EC, which are preferably XOR operations as well. They combine the left-hand data LD_1 and the right-hand data RD_1, respectively, which originate from the preparatory operation (PP), with a zeroth auxiliary value A_0 and a first auxiliary value A_1. The results of the combinatory operations DC and EC are left-hand masked data LD'_1 and right-hand masked data RD_1', respectively (*in the continuation of this text, masked data will be designated by an apostrophy*). The maskings make themselves felt in the subsequent steps. Since the left-hand data of the second step S_2 is equal to the masked right-hand data of the first step S_1, said left-hand data LD'_2 is masked as well. The right-hand data RD_2' of the second step is masked since it is equal to the masked, modified data SD_1'.

Combining the data LD_i and RD_i with the auxiliary values A_i therefore results in the modified data LD_i' and RD_i' being masked, as a result of which it is considerably more difficult to derive the original data X or the key used from the masked data LD_i' and RD_i'.

In order to remove the auxiliary values A_i prior to the final operation (PP^{-1}), there are provided completing combinatory operations FC and GC, which combine the modified and masked left-hand data SD'_n of the last step S_n with an auxiliary value A_{n+1} and the masked right-hand data RD_n' with an auxiliary value A_n, respectively. On account of $A_i \oplus A_i$ being zero in this manner the maskings are removed by the auxiliary values A_i. As a result, it is possible to carry out the method in such a manner that, notwithstanding the use of the auxiliary values A_i, the final data Y is equal to that which would have been obtained by the conventional method according to FIG. 5.

In order to exclude the effect of the auxiliary values A_i on the results FD_i of the operations F_i, in each step S_i there is preferably present a supplementary combinatory operation AC_i which combines the right-hand data RD_i with a (primary) auxiliary value A_i before this data is fed to the cryptographic operation F_i. The result of each supplementary combinatory operation AC_i is non-masked right-hand data RD_i, so that the cryptographic operation F_i works on the same data as in the process of FIG. 5.

There may be advantageously inserted a further combinatory operation BC_i between the cryptographic operation F_i and the combinatory operation CC_i with the purpose of combining the processed (right-hand) data FD_i with a further (secondary) auxiliary value B_i. As a result, there may be achieved a masking of the processed data FD_i and a further masking of the (modified) left-hand data SD_i'. The combinatory operations AC_i and BC_i preferably are XOR operations as well.

In accordance with a further aspect of the invention, the auxiliary values A_i and B_i are related. The secondary auxiliary values B_i are formed, preferably using an XOR operation, from the first auxiliary value A_{i-1} of the previous step and the auxiliary value A_{i+1} of the next step:

$$B_i = A_{i-1} \oplus A_{i+1}.$$

This results in each primary auxiliary value A_{i+1} which, using a further supplementary combinatory operation BC_i, is combined with the processed right-hand data FD_i as an ingredient of the secondary auxiliary value B_i, repeatedly being compensated in the next step, i.e., step S_{i+1}, by means of a combinatory operation AC_i before the right-hand data RD_{i+1} is subjected to the operation F_i. The (masked) right-hand data RD_i' in question, which forms the (masked) left-hand data LD_{i+1}' of the still next step S_{i+2} are combined there with the primary auxiliary value A_{i+1} and is compensated in this manner. The auxiliary value A_{i+1} makes itself felt in the modified data SD_i', in such a manner that this remains masked between two steps.

The left-hand data LD_1 of the first step S_1 is masked with the additional or zeroth (primary) auxiliary value A_0. By combining, with the secondary auxiliary value $B_1 = A_0 \oplus A_2$, the initial auxiliary value A_0 is removed (on account of $A_0 \oplus A_0$ being zero), but the auxiliary value A_2 and the masking achieved therewith are maintained. The zeroth auxiliary value A_0 in this embodiment is preferably chosen equal to the first auxiliary value A_1.

Although all primary auxiliary values A_i are preferably chosen different, with the exception of $A_0 = A_1$, it is possible to choose all primary auxiliary values A_i equal. In this case, all secondary auxiliary values B_i in the embodiment shown will be equal to zero, so that the further combinatory operations BC_i may be omitted. The invention further applies to processes P which contain only one step S, or have a deviating structure.

In the process of FIG. 7, which largely corresponds to that of FIG. 6, the combinatory operations AC_i and BC_i and the cryptographic operation F_i in each step are integrated to form a combined operation F_i'. Integrating the combinatory operations in the operations F_i is possible by suitably adjusting, e.g., a substitution table of the operation F_i. As a result, the supplementary combinatory operations AC_i and BC_i may be omitted and the result of the adjusted operation F_i' is equal to the result of the total of the operation F_i proper and the combinatory operations:

$$FD_i' = F_i'(RD_i') = B_i \oplus F_i\ (A_i \oplus RD_i').$$

Basically, each step S_i requires a different combinatory operation F_i in which various auxiliary values A_i are integrated (see FIG. 6). Only if the auxiliary values A_i are chosen equal, i.e., $A_1=A_2 = \ldots = A_n$, the combinatory operations F_i in this embodiment may be equal.

Each time the process is carried out, the values A_i are preferably chosen anew. For the process of FIG. 7, this means that the combined operations F_i' are then determined anew. Since the operations F_i' in many implementations will comprise the use of several tables, such as substitution tables, said tables will be determined anew each time the process P is carried out. In order to offer a supplementary protection against attacks, according to a further aspect of the invention the tables will be determined in random order. If a combined operation F_i' comprises, e.g., eight tables, said eight tables will be determined in another order each time said operation F_i' is carried out anew. Said order may be determined on the basis of the contents of an order register, which contents may each time be formed by a random number originating from a random-number generator. On the basis of the contents of the order register there may each time be composed a fresh lookup table. Using the lookup table, the tables may be written to a memory and later be read out.

According to a further aspect of the invention, supplementing this or instead thereof, the elements of each table may be determined and/or stored in random order. With this measure it is achieved that the protection against attacks is also improved. In this case, too, there may be applied a lookup table on the basis of which the elements may later be retrieved.

The measures referred to above may also be applied in another embodiment of the invention, such as the one of FIG. 8,

or in completely different other processes, whether cryptographic or not.

The embodiment of FIG. 8 largely corresponds to that of FIG. 7. Supplementing FIG. 7, each step S_i, with the exception of the last step S_n, includes a combinatory operation HC_i which combines the right-hand data RD_i with a tertiary auxiliary value W_i. The tertiary auxiliary value W_i preferably equals the XOR combination of the auxiliary values A_0 and A_1:

$$W = A_0 \oplus A_1,$$

where $A_0 \neq A_1$.

This results in the operation HC_i always adding the zeroth auxiliary value A_0 and compensating the first auxiliary value A_1. As a result, it is possible that all cryptographic operations F_i are essentially identical, which requires a much smaller processing and/or storage capacity from a processor system with which the method is carried out. In the embodiment of FIG. 8, the operations F_i" are such adjustments of the original operations F_i, that these are corrected for the auxiliary value A_1 and in addition combine the tertiary auxiliary value $W = A_0 \oplus A_1$ with their result. In other words, if $RD_i \oplus A_1$ is fed to F", the result will be equal to

$FD_i' = F_i(RD_i) \oplus W$.

It will be understood by those skilled in the art that the combinatory processes AC_i, BC_i and HC_i may be carried out in different locations in the cryptographic process P to achieve a comparable or even identical effect.

FIG. 9 schematically shows a circuit 10 for implementing the method according to the invention. The circuit 10 comprises a first memory 11, a second memory 12 and a processor 13, the memories 11 and 12 and the processor 13 being coupled using a data bus 14. By providing two memories, it is possible each time to carry out a substep of one of the processes P and P* (see FIG. 4), to store the result of said substep in, e.g., the first memory 11, and from the second memory 12 to transfer a previous interim result from the other process to the processor 13. In this manner, it is possible to efficiently carry out the alternating computation of substeps of two different processes.

The payment system schematically shown in FIG. 10 comprises an electronic payment means 1 and a payment station 2. The electronic payment means 1 is, e.g., a so-called smart card,

i.e., a card provided with an integrated circuit for storing and processing payment data. The payment station 2 comprises a card reader 21 and a processor circuit 22. The processor circuit 22 may correspond to the circuit 10 of FIG. 9.

At the beginning of a transaction, the payment means 1 transmits an identification (card identification) ID to the payment station 2. By reference to said identification, the payment station 2 determines a key which will be used for said transaction. Said identification ID may be fed as input data X (see the figures 1-3) to a cryptographic process which, on the basis of a master key MK, produces an identification-dependent transaction key K_{ID} as output data Y. In accordance with the invention, for this purpose the process shown in the figures FIG. 2 and 3 is used, the master key MK having been converted in advance, using a process R, into a supplementary master key MK*. Said supplementary master key MK* is now fed, preferably together with the identification ID, in accordance with FIG. 3, to the supplementary process P* in order to reproduce the original master key MK and to derive the transaction key K_{ID} from the identification ID.

Although, in the figures FIG. 2 and 3, there is always shown one single supplementary process P*, there may possibly be used several processes P*, P**, P***, ... in series and/or in parallel to derive the primary key K.

It will be understood by those skilled in the art that many modifications and amendments are possible without departing from the scope of the invention.

CLAIMS

1. Method for cryptographically processing data, comprising feeding, to a cryptographic process (P), values, namely, the data (X) and a key (K), and carrying out the process (P) in order to form cryptographically processed output data (Y), characterised by feeding, to the process (P), auxiliary values (K*; A, B) and compensating, by an auxiliary process, the influence of the auxiliary values to the output data, in order to mask the values (K; D) used in the process (P).

2. Method according to claim 1, wherein an auxiliary value comprises a supplementary key (K*) which is fed to a supplementary process (P*) in order to form the key (K).

3. Method according to claim 2, wherein the supplementary process (P*) comprises a cryptographic process to which an auxiliary key (K') is fed.

4. Method according to claim 2 or 3, wherein the supplementary process (P*) is an invertible process.

5. Method according to claim 2, 3 or 4, wherein the data (X) is also fed to the supplementary process (P*).

6. Method according to claim 5, wherein carrying out the supplementary process (P*) takes place exclusively if the data (X) has predetermined properties.

7. Method according to any of the claims 2-6, wherein the process (P) and the supplementary process (P*) each are built up from a number of steps, and wherein steps of the process (P) and the supplementary process (P*) are alternated.

8. Method according to any of the preceding claims, wherein the process (P) comprises a number of steps (S_i), each having a cryptographic operation (F_i, F_i', F_i'') for processing right-hand data (RD_i) derived from the data (X) and a combinatory operation (C_i) for combining with left-hand data (LD_i) also derived from the data (X), the processed right-hand data (FD_i) in order to form modified left data (SD_i), and wherein the right-hand data (RD_1) is combined with a primary auxiliary value (A_1) prior to the first

9. Method according to claim 8 wherein, immediately after the last step (S_n), the right-hand data (RD_n) is combined with a further primary auxiliary value (A_n) and the modified left-hand data (SD_n') is combined with a further additional auxiliary value (A_{n+1}).

10. Method according to claim 8 or 9, wherein the right-hand data (RD_i) is combined, in each step (S_i) and prior to the operation (F_i'), with the primary auxiliary value (A_i) of said step (S_i).

11. Method according to claim 10, wherein the processed right-hand data (FD_i) is combined, following the operation (F_i), with the secondary auxiliary value (B_i) of said step (S_i).

12. Method according to claims 10 and 11, wherein the secondary auxiliary value (B_i) of a step (S_i) is formed from the combination of the primary auxiliary value (A_{i-1}) of the preceding step and the primary auxiliary value (A_{i+1}) of the next step.

13. Method according to any of the claims 8-12, wherein all primary auxiliary values (A_i) are equal.

14. Method according to any of the claims 9-13, wherein the primary auxiliary values (A_i) and/or secondary auxiliary values (B_i) have each time been combined with the respective operation (F_i) in advance.

15. Method according to claim 14, wherein a combined operation (F_i') contains several tables, and wherein the tables are determined in a different order each time the process (P) is carried out.

16. Method according to claim 14 or 15, wherein a combined operation (F_i') contains several tables, and wherein the elements of the tables are determined and/or stored in a different order each time the process (P) is carried out.

17. Method according to claim 16, wherein the order is stored as a lookup table for the benefit of reading out the elements.

18. Method according to any of the claims 8-17, wherein the right-hand data (RD_i) is combined with a tertiary auxiliary value (W_i) after each step (S_i).

19. Method according to claim 18, wherein the tertiary auxiliary value (W_i) in all steps, except the last one (S_n) is equal to the combination of the primary auxiliary value (A_1) of the first step (S_1) and the additional auxiliary value (A_0), and in the last step (S_n) is equal to zero.

20. Method according to any of the claims 8-19, wherein combining is carried out using an XOR operation.

21. Method according to any of the preceding claims, wherein the data (X) comprises identification data of a payment means (1) and the processed data (Y) forms a diversified key.

22. Method according to any of the preceding claims, wherein the process (P) comprises DES, preferably triple DES.

23. Circuit (10) for carrying out the method according to any of the preceding claims.

24. Payment card (1), provided with a circuit (10) according to claim 23.

25. Payment terminal (2) provided with a circuit (10) according to claim 23.

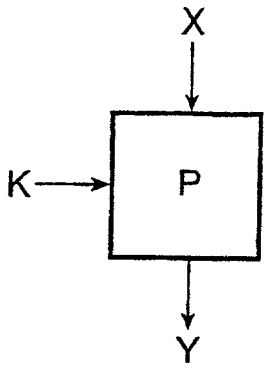

FIG. 1

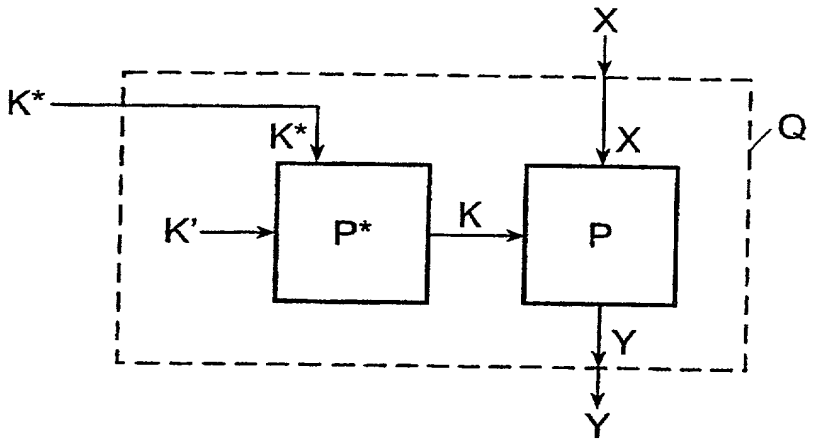

FIG. 2

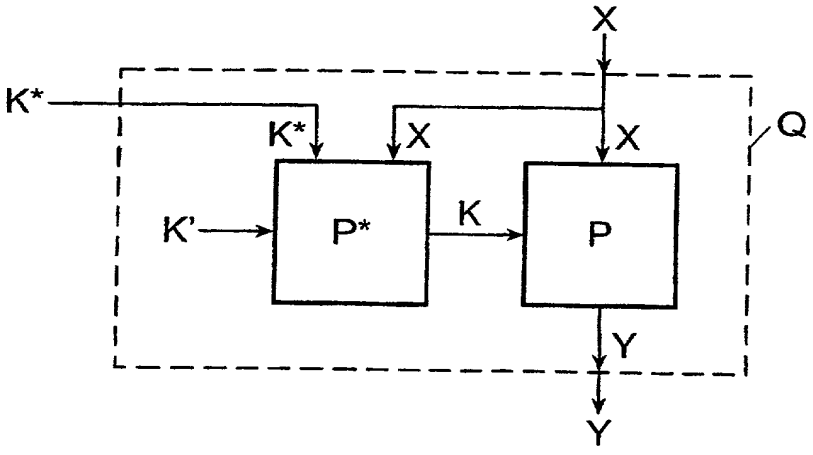

FIG. 3

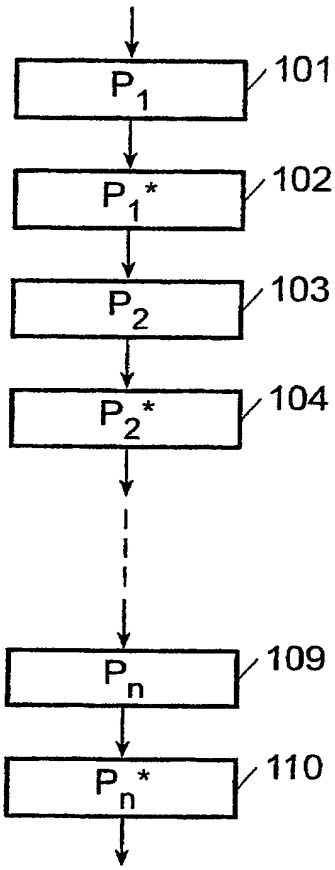

FIG. 4

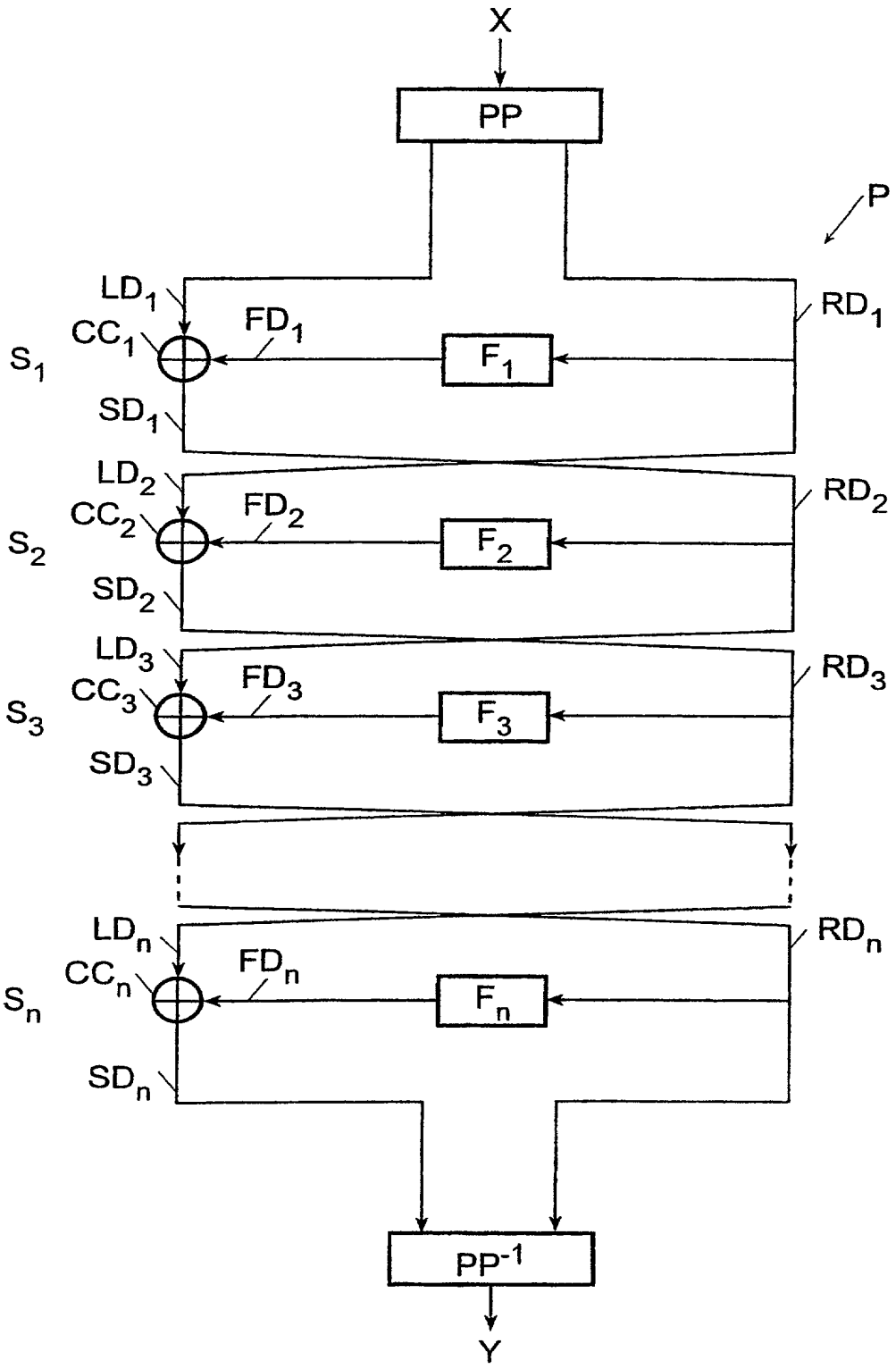
X
PP
P
LD1
CC1
FD1
F1
RD1
S1
SD1
LD2
CC2
FD2
F2
RD2
S2
SD2
LD3
CC3
FD3
F3
RD3
S3
SD3
LDn
CCn
FDn
Fn
RDn
Sn
SDn
PP-1
Y

FIG. 5

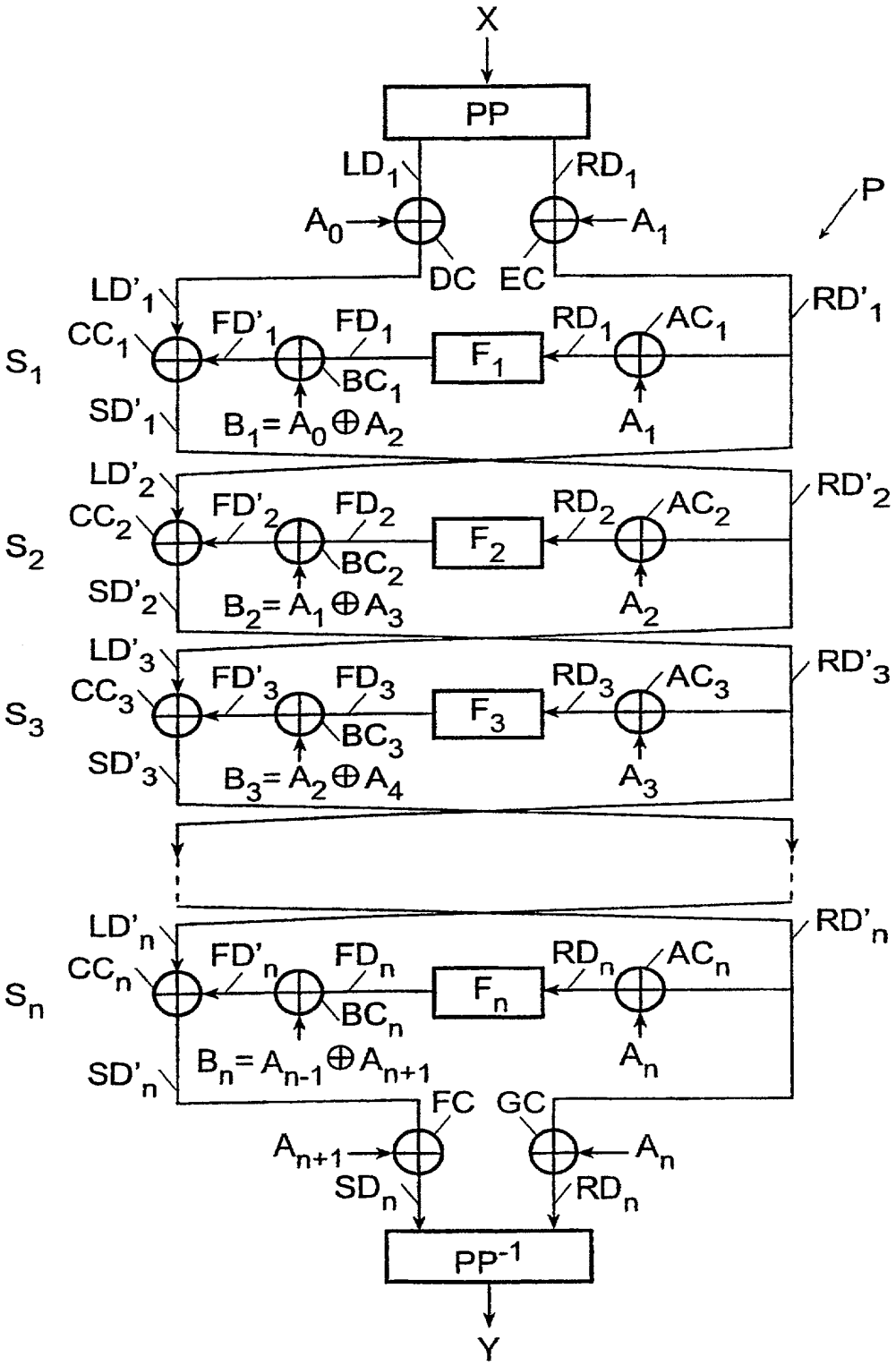
X
PP
LD1
RD1
A0
A1
P
DC
EC
LD'1
RD'1
CC1
FD'1
FD1
RD1
AC1
S1
F1
BC1
SD'1
B1= A0 ⊕ A2
A1
LD'2
RD'2
CC2
FD'2
FD2
RD2
AC2
S2
F2
BC2
SD'2
B2= A1 ⊕ A3
A2
LD'3
RD'3
CC3
FD'3
FD3
RD3
AC3
S3
F3
BC3
SD'3
B3= A2 ⊕ A4
A3
LD'n
RD'n
CCn
FD'n
FDn
RDn
ACn
Sn
Fn
BCn
SD'n
Bn= An-1 ⊕ An+1
An
FC
GC
An+1
An
SDn
RDn
PP-1
Y

FIG. 6

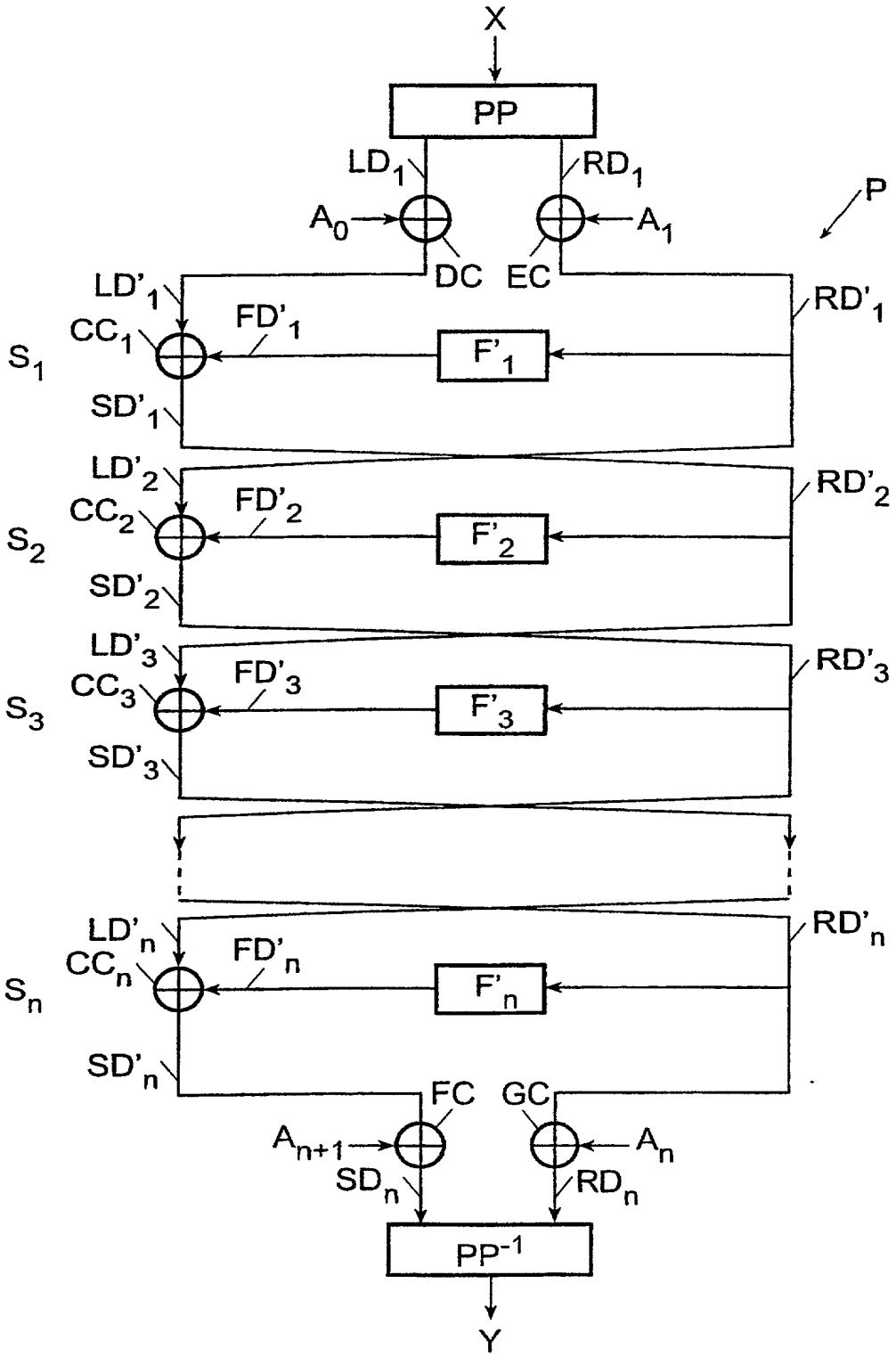

FIG. 7

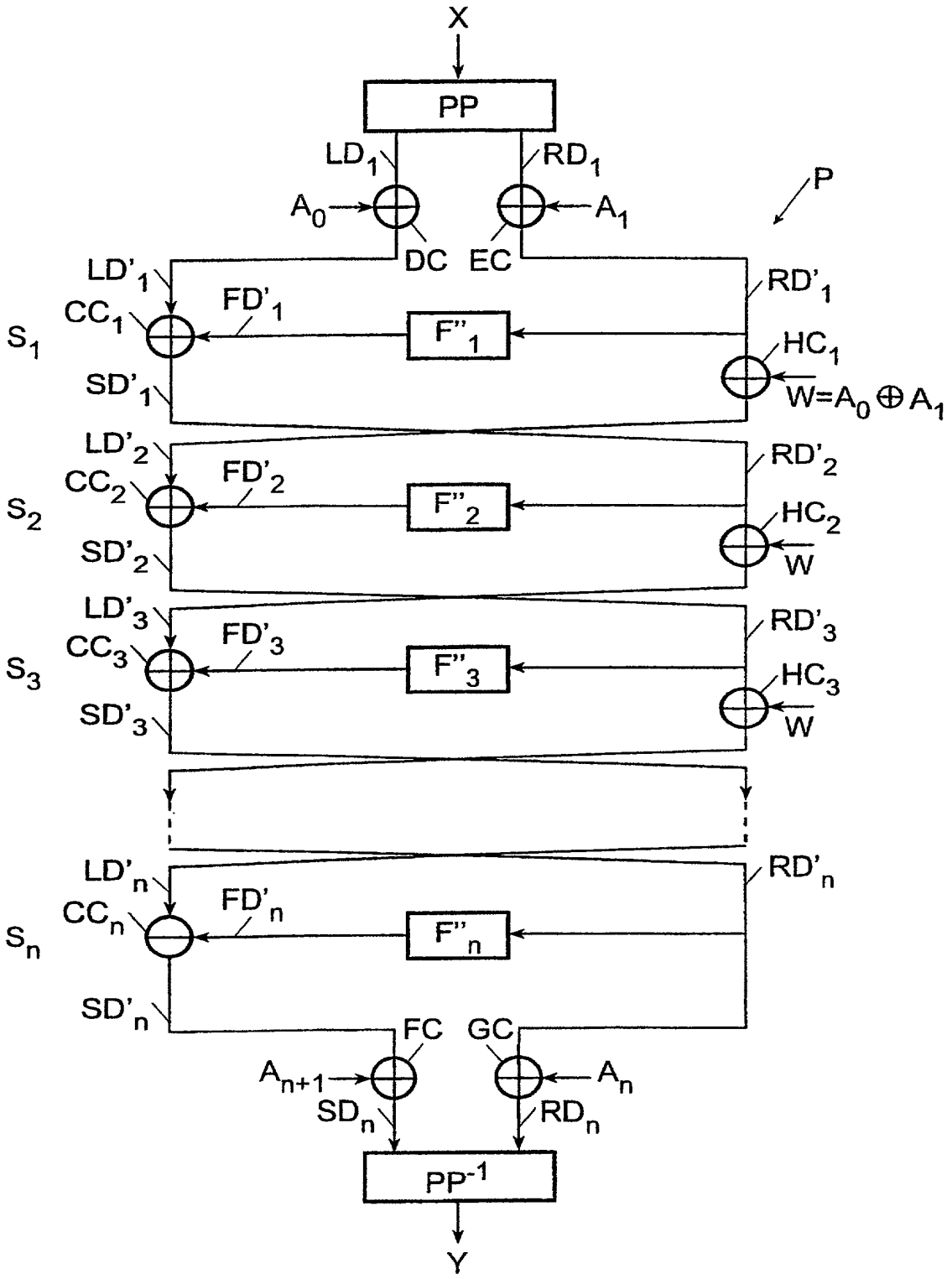
X
PP
LD1
RD1
A0
A1
P
DC
EC
LD'1
RD'1
FD'1
CC1
F"1
S1
HC1
SD'1
W=A0 ⊕ A1
LD'2
RD'2
FD'2
CC2
F"2
S2
HC2
SD'2
W
LD'3
RD'3
FD'3
CC3
F"3
S3
HC3
SD'3
W
LD'n
RD'n
FD'n
CCn
F"n
Sn
SD'n
FC
GC
An+1
An
SDn
RDn
PP-1
Y

FIG. 8

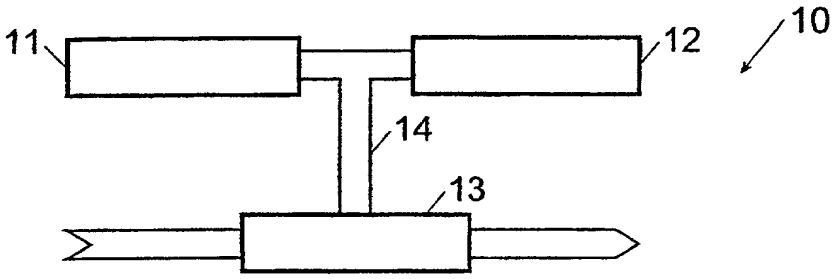

FIG. 9

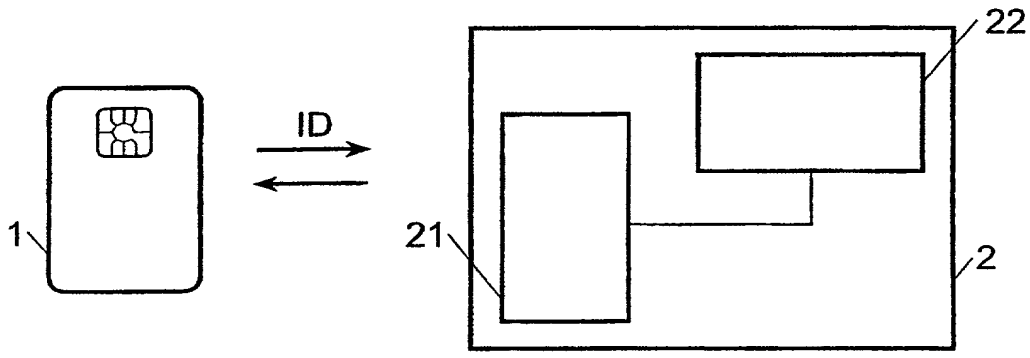

FIG. 10

Power of attorney:

As a named inventor, I hereby appoint:

Peter L. Michaelson (Reg. No. 30,090)
Robert M. Wallace (Reg. No. 29,119)
Jeremiah G. Murray (Reg. No. 20,533)
John T. Peoples (Reg. No. 28,250)
Ronald L. Drumheller (Reg. No. 25,674)
Edward M. Fink (Reg. No. 19,640)
Christopher Balzan (Reg. No. 40,901)
Eric Agaard (Reg. No. 40,478)

as my attorneys to prosecute this application and to transact all business in the United States Patent and Trademark Office in connection therewith.

Direct all correspondence to Customer Number 007265 at the following address:

MICHAELSON & WALLACE
Parkway 109 Office Center
328 Newman Springs Road
P.O. Box 8489
Red Bank, New Jersey 07701.

Direct all telephone calls to: (732) 530-6671.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Atty. Doc. No.: _____

DECLARATION AND
POWER OF ATTORNEY
(Utility Patent Application)

As a below named inventor, I hereby declare:

My residence, post office address and citizenship are as stated below next to my name,

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below), of the subject matter which is claimed and for which a patent is sought on the invention entitled:
"Method and device for cryptographically processing data."

the specification of which:

__ is attached hereto
__ was filed on _____ as Application Serial No. _____ with amendment(s) filed _____
X was filed as PCT international application: serial number PCT/EP99/10208 on December 16, 1999 and was amended on November 25, 2000.

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose information which is material to the patentability of this application in accordance with Title 37, Code of Federal Regulations section 1.56.

I hereby claim foreign priority benefits under Section 119 of Title 35, United States Code for the above-identified US patent application based on the patent or inventor's certificate identified below and having a filing date before that of the US patent application for which priority is claimed:

Application No.	Country	Filing Date	Priority Claimed under 35 USC 119
1010921	NL	December 30, 1998	YES
1011544	NL	March 12, 1999	YES
1011800	NL	April 15, 1999	YES

I hereby claim the benefit under Section 120 and/or Section 119(e) of Title 35 of the United States Code of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by Section 112 of Title 35 of the United States Code, I acknowledge the duty to disclose material information, as defined in Section 1.56 of Title 37 of the Code of Federal Regulations, which occurred between the filing date of the prior application and the national or PCT international filing date of this application:

Application Serial No.	Filing Date	Status: Patented	Pending	Abandoned

100 First inventor:

Full name: ROELOFSEN (last) Gerrit (first)

Residence address: Rijndijk 60-A (Street)

2331 AH (zip code) LEIDEN (state) NLY The Netherlands (country)

Post Office address: P.O.Box 95321 (post office & box number)

2509 CH (zip code) THE HAGUE (state) The Netherlands (country)

Citizenship: The Netherlands (country)

Signature: _____

Date: 27 02 2001

Second inventor:

Full name: VAN BRUCHEM (last) Dirk (first) Jan Jacobus (middle)

Residence address: Randveen 4
Street

2291 NM (zip code) Wateringen (state) The Netherlands (country)

NLX

Post Office address: P.O. Box 95321
post office & box number

2509 CH (zip code) THE HAGUE (state) The Netherlands (country)

Citizenship: The Netherlands
Country

Signature: _____

Date: 5-3-2001

300 Third inventor:

Full name: MULLER (last) Frank (first) (middle)

Residence address: Meerkoetlaan 24
Street

2623 NJ DELFT NLX The Netherlands
zip code state country

Post Office address: P.O. Box 95321
post office & box number

2509 CH THE HAGUE The Netherlands
zip code state country

Citizenship: The Netherlands
Country

Signature: _____

Date: 27-2-'01

400

Fourth inventor:

Full name: ROMBAUT (last) Willem (first) (middle)

Residence address: C.A. van Beverenplein 11
Street

2552 HT (zip code) THE HAGUE (state) NLX The Netherlands (country)

Post Office address: P.O. Box 95321
post office & box number

2509 CH (zip code) The Hague (city) The Netherlands (country)

Citizenship: The Netherlands
Country

Signature: _____

Date: 5-3-2001